平成１８年度　第１回
電気通信主任技術者試験問題

午前の部
法規・設備及び設備管理

注　意　事　項

1　試験開始時刻　　**１０時００分**

2　試験科目別終了時刻

試　験　科　目	科目数	終　了　時　刻
「法規」のみ	1 科目	**１１時２０分**
「伝送交換設備(又は線路設備)及び設備管理」のみ	1 科目	**１１時４０分**
「法規」及び「伝送交換設備(又は線路設備)及び設備管理」	2 科目	**１３時００分**

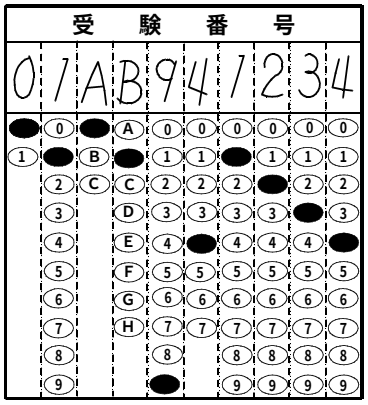
3　試験種別と試験科目別の問題(解答)数及び試験問題ページ

試　験　種　別	試　験　科　目	問　題　(　解　答　)　数					試験問題
		第1問	第2問	第3問	第4問	第5問	ペ　ー　ジ
伝送交換主任技術者	法　規	7	7	7	7	6	1～15
	伝送交換設備及び設備管理	8	8	8	8	8	16～28
線路主任技術者	法　規	7	7	7	7	6	1～15
	線路設備及び設備管理	8	8	8	8	8	29～39

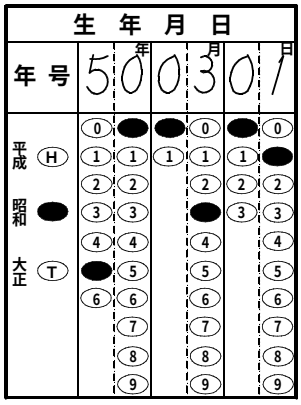
4　受験番号等の記入とマークの仕方

(1) **マークシート(解答用紙)にあなたの受験番号、生年月日及び氏名をそれぞれ該当枠に記入してください。**
(2) **受験番号及び生年月日に該当する箇所を、それぞれマークしてください。**
(3) **生年月日の欄は、年号をマークし、生年月日に１けたの数字がある場合、十の位のけたの「0」もマークしてください。**

[記入例]　受験番号　０１ＡＢ９４１２３４



生年月日　昭和５０年3月1日



5　答案作成上の注意

(1) **マークシート(解答用紙)は１枚で、２科目の解答ができます。**
「法規」は赤色(左欄)、「伝送交換設備(又は線路設備)及び設備管理」(「設備及び設備管理」と略記)は緑色(右欄)です。
(2) **解答は試験科目の解答欄の正解として選んだ番号マーク枠を、黒の鉛筆(ＨＢ又はＢ)で濃く塗りつぶしてください。**
① **ボールペン、万年筆などでマークした場合は、採点されません**ので、使用しないでください。
② **一つの問いに対する解答は一つだけです。**二つ以上マークした場合、その問いについては採点されません。
③ **マークを訂正する場合は、プラスチック消しゴムで完全に消してください。**
(3) **免除の科目がある場合は、**その**科目欄は記入しない**でください。
(4) **受験種別欄は、**あなたが**受験申請した試験種別**を○で囲んでください。(試験種別は次のように略記されています。)
① 伝送交換主任技術者は、　　**『伝 送 交 換』**
② 線路主任技術者は、　　**『線　　路』**

6　合格点及び問題に対する配点

(1) 各科目の満点は１００点で、合格点は６０点以上です。
(2) 各問題の配点は、設問文の末尾に記載してあります。

7　登録商標などに関する事項

(1) 試験問題に記載されている会社名又は製品名などは、それぞれ、各社の商標または登録商標です。
(2) 試験問題では、® 及び ™ を明記していません。
(3) 試験問題の文中及び図中などで使用しているデータは、すべて架空のものです。

マークシート(解答用紙)は、絶対に折り曲げたり、汚したりしないでください。

次ページ以降は試験問題です。試験開始の合図があるまで、開かないでください。

受験番号(控え)										

(今後の問い合わせなどに必要になります。)

試　験　種　別	試　験　科　目
伝送交換主任技術者	伝送交換設備及び設備管理

問１　次の問いに答えよ。　(小計２０点)

(１)　次の文章は、高速大容量の光伝送システムの概要について述べたものである。［　　］内の(ア)～(エ)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、［　　］内の同じ記号は、同じ解答を示す。　(２点×４＝８点)

トラヒックの増加に伴うネットワークの高速、大容量化を実現するため、波長多重(ＷＤＭ)技術の適用などが進められている。

光伝送システムは、波長数の増加及び［（ア）］という二つの技術により更に大容量化を図ることが可能である。波長数増加のための方法の一つとして、新規の波長帯を用いる光信号の伝送があり、長距離の中継伝送を行うには、［（イ）］の開発が必要である。

ＩＴＵ－Ｔでは、次世代の伝送網としてＯＴＮの勧告化が進められている。ＯＴＮでは、波長単位での多重分離や通信路設定が行われることになり、従来の伝送装置ではなく、ＯＸＣやＯＡＤＭが主に用いられることになる。ＳＤＨ、ＡＴＭ、イーサネットなどの信号は、［（ウ）］といわれるフレームに収容され、ＯＴＮ内をエンド・ツー・エンドで伝送される。

［（ウ）］のフレームフォーマットには、ＳＤＨ同様、保守や運用管理に必要な情報の転送を行うためのオーバーヘッドが含まれている。また、［（ウ）］のフレームには、これまで主にＡＴＭ方式などで適用されてきた［（エ）］が付加され、より信頼性の高い信号伝送を可能としている。

<(ア)～(エ)の解答群>

①　ＦＥＣ	②　ＯＣｈ	③　ＯＭＳ	④　ＯＴＳ
⑤　ＳＴＭ	⑥　ＳＯＨ	⑦　ポインタ	⑧　ラベル

⑨　波長当たりの伝送容量の増加　　⑩　光送信機の高出力化
⑪　使用する光ファイバの低損失化　　⑫　波長多重・分離回路の高速化
⑬　ダイナミックレンジの広い光受信装置
⑭　新規波長帯で分散が０となる光ファイバ
⑮　新規波長帯で動作する光ファイバ増幅器

(2) 次の文章は、ＶｏＩＰ(Voice over Internet Protocol)の概要について述べたものである。［　　］内の(オ)、(カ)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。
(3点×2＝6点)

(i) ＶｏＩＰのシグナリング、符号化技術について述べた次の文章のうち、正しいものは、［(オ)］である。

<(オ)の解答群>

① 音声信号の符号化方式には、主に、ＩＴＵ－Ｔ勧告Ｇ.７１１、Ｇ.７２９ａなどが用いられている。Ｇ.７１１はＰＣＭによる符号化方式で、音声信号を６４〔kbit／s〕のディジタル信号に変換する。Ｇ.７２９ａは、ＣＳ－ＡＣＥＬＰ(Conjugate Structure Algebraic Code Excited Linear Prediction)による符号化方式で、音声信号を１６〔kbit／s〕のディジタル信号に変換する。

② ＶｏＩＰで使用される主な呼制御プロトコルには、ＩＴＵ－Ｔ勧告のH.３２３、H.２４８、ＩＥＴＦ標準のＳＩＰ(Session Initiation Protocol)、ＩＥＥＥの標準規格８０２.１Ｑなどがある。

③ ＣＳ－ＡＣＥＬＰは、コードブックに登録された波形パターンの番号と、過去に入力された音声信号から予測される音響特性(フィルタ係数)を送信する方式である。

④ ＳＩＰは、基本的にバイナリ値(２進数)ベースでパラメータを追加できるため、テキストベースでのやりとりを行うH.３２３と比較して、機能の拡張が容易である。

⑤ ＳＩＰは、ＯＳＩ参照モデルのプレゼンテーション層の上位レイヤに位置づけられ、そのレイヤの下位であるプレゼンテーション層とは独立にセッションを生成、変更、終了する機能を有している。

(ii) ＶｏＩＰにおける音声信号のパケット化、プロトコルなどについて述べた次の文章のうち、誤っているものは、［(カ)］である。

<(カ)の解答群>

① 音声信号のパケット化においては、符号化された音声信号にヘッダが付加される。ヘッダの種類には、ＩＰヘッダ、ＵＤＰヘッダ、ＲＴＰヘッダがある。

② ＲＴＰヘッダの機能には、同期タイミングを合わせる機能及びＱｏＳ制御機能がない。このため、シーケンス番号に応じたデータ再構成やタイミング制御を行う機能が別途に必要である。

③ ＲＴＰヘッダは、音声パケットのペイロードに対する付加情報を与える役割を持ち、その内容はシーケンス番号、タイムスタンプ、ペイロードタイプ、同期送信元識別子及び寄与送信元識別子などで構成される。

④ ＶｏＩＰでは、音声データの転送に高い即時性が必要となり、即時性を実現するため、トランスポート層のプロトコルにはＴＣＰが使用されている。ＴＣＰは、ＵＤＰで実行されるＩＰパケットの送達確認、フロー制御、再送確認機能を持たないため、ＵＤＰと比較してパケット処理に要する時間が短い。

⑤ ＲＴＰヘッダのタイムスタンプは実時間性の保証に使用され、シーケンス番号はパケットの順序制御に使用される。

（３） 次の文章は、ＩＰｖ６について述べたものである。 [　　] 内の(キ)、(ク)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。 （３点×２＝６点）

（ｉ） ＩＰｖ６について述べた次の文章のうち、正しいものは、 [（キ）] である。

<(キ)の解答群>

① ＩＰアドレス空間として１２８ビットが割り当てられ、この１２８ビットを１６ビットずつに区分し、区分された一つ一つを１０進数で表記したものをカンマで結んでアドレスとして表記される。

② 基本ヘッダには、トラヒッククラス、フローラベル、ペイロード長、ホップ制限、認証ヘッダ、暗号ペイロードヘッダなどのフィールドがある。

③ ＩＰｖ６のヘッダには、送信元ＩＰアドレス及びあて先ＩＰアドレスを合わせて１２８バイトのフィールドが割り当てられている。

④ ＩＰｖ６のヘッダは、４０バイトの固定長の基本ヘッダと必要により付加される拡張ヘッダにより構成される。

（ⅱ） ＩＰｖ６の特徴、機能などについて述べた次の文章のうち、誤っているものは、 [（ク）] である。

<(ク)の解答群>

① セキュリティ機能として、通信内容の暗号化、通信相手の認証などがあり、暗号化には、共通鍵暗号アルゴリズムなどが利用される。

② ＩＰヘッダの誤りチェックを行うためのヘッダチェックサムフィールド、１６ビット長が規定されている。

③ 基本ヘッダと拡張ヘッダの機能分離により、ヘッダの簡素化と拡張性が確保されている。

④ ＩＰｖ６パケットの前にＩＰｖ４ヘッダを付けてカプセル化し、ＩＰｖ４ネットワークをトンネリングさせることができる。

⑤ フローラベルフィールドの追加により、ルータにおけるフロー検出処理が、ＩＰｖ４と比較して簡便になり、ＱｏＳの実現が容易となる。

問２　次の問いに答えよ。　　(小計２０点)

(１)　次の文章は、衛星通信システムについて述べたものである。［　　］内の(ア)～(エ)に最も適したものを、下記の解答群から選び、その番号を記せ。　　(２点×４＝８点)

静止衛星による衛星通信システムは、地球の自転周期と一致する赤道上空、約３６,０００〔km〕の軌道に打ち上げられた衛星を用いた通信システムである。この静止衛星通信システムは、地上の災害の影響を受けにくいという高い災耐性のほか、広範な衛星照射エリアを活かした［(ア)］という特徴を有する。また、地球局相互間には、約［(イ)］〔ms〕程度の空間伝搬遅延が生ずるという特徴もある。

衛星通信システムに使用される周波数帯は、衛星通信システム相互間及び［(ウ)］などを考慮して決定され、［(エ)］において分配されている。

<(ア)～(エ)の解答群>

①　３　　②　３０　　③　３００　　④　ＩＳＯ　　⑤　ＩＥＴＦ
⑥　ＩＥＥＥ　　⑦　ＩＴＵ　　⑧　同報性　　⑨　局地性　　⑩　閉域性
⑪　地球局における太陽雑音の妨害　　⑫　地上無線通信方式との干渉条件
⑬　宇宙局における地球による日食の影響

(２)　次の文章は、ディジタル伝送技術の概要について述べたものである。［　　］内の(オ)、(カ)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。　(３点×２＝６点)

(ｉ)　音声信号の符号化方式などについて述べた次の文章のうち、誤っているものは、［(オ)］である。

<(オ)の解答群>

①　時間的に連続なアナログ信号をディジタル信号に変換する場合は、一般的に、標本化→量子化→符号化という順序により行われる。
②　一般の音声伝送では、４kHz帯域の音声信号を標本化周波数８〔kHz〕で標本化し、それぞれの標本値を８〔bit〕で符号化するもので、音声１チャネルは、６４〔kbit／s〕で符号化される。
③　量子化の過程では、ある範囲内の標本値は、同一の符号列で表現されるため、受信側では、すべて同一の振幅として復号される。このため、送信と受信の信号では本質的に誤差が発生する。この誤差に基づく雑音は量子化雑音といわれる。
④　１標本当たりの符号化ディジット数を１〔bit〕増加することにより、信号対量子化雑音比は３〔ｄＢ〕改善される。
⑤　非直線量子化の圧伸特性には、μ-ｌａｗやA-ｌａｗがある。

(ⅱ) 高能率音声符号化技術、画像符号化技術について述べた次の文章のうち、正しいものは、［（カ）］である。

<(カ)の解答群>

① ＣＶＳＤ方式は、適応予測と適応量子化を使用する差分ＰＣＭ方式であり、６４〔kbit／s〕帯域を２回線として使用することができる。

② 音声信号の高能率符号化方式には、音声の生成過程を分析合成する生成源符号化方式と音声波形の冗長度を除いて符号化する波形符号化方式があり、生成源符号化方式は、一般に、ボコーダといわれる。

③ 画像符号化方式には、フレーム間予測符号化方式が用いられ、原理的に予測が不可能なフレーム内予測符号化方式は適用されない。

④ ＭＰＥＧ－１は、ＩＴＵ－Ｔ勧告による１．５〔Mbit／s〕以下の伝送帯域での蓄積メディアなどに用いられる静止画像符号化方式である。

(３) 次の文章は、通信用電源設備について述べたものである。［　　］内の(キ)、(ク)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。（３点×２＝６点）

(ｉ) エンジン発電装置について述べた次の文章のうち、正しいものは、［（キ）］である。

<(キ)の解答群>

① すべてのディーゼル機関は冷却水が必要なため、山上、離島などの冷却水が得にくい場所には使用されない。

② エンジン発電装置に使用されている主要な内燃機関は、ガスタービンとディーゼル機関である。ガソリン機関は、構造が複雑で長時間の運転に難点があるため、エンジン発電装置の内燃機関には用いられていない。

③ ガスタービンは、ディーゼル機関と同様に、冷却水を必要とするが、単位時間・出力当たりの燃料消費量はディーゼル機関と比較して少なく、また、小型軽量に構成できる利点を有している。

④ エンジン発電装置と組み合わせて使用される太陽光発電方式において、十分な太陽光エネルギーの得られる時間は、太陽電池モジュールの出力を直接、負荷に供給し、夜間など、太陽電池モジュールの出力が停止すると同時に、エンジン発電装置が起動され、その出力が負荷に供給される。

⑤ エンジンに直結される発電機には、一般に、交流発電機が用いられ、電圧、周波数の自動調整機能を具備しているものがある。

(ⅱ) 受電装置に使用されている機器について述べた次の文章のうち、誤っているものは、［（ク）］である。

<(ク)の解答群>

① 一般に、受電用として用いられている変圧器は、構造上から外鉄型と内鉄型に、絶縁・冷却方式からは油入式と油を使用しない乾式に、相数からは単相式と３相式に分類される。

② 遮断器は電路の遮断の際に発生するアークの消去方式により、油入遮断器、空気遮断器などがある。

③ 遮断器には規定の条件のもとでその性能を保証するため、定格が決められている。主なものは、定格電圧、定格電流、定格最大電流、定格最大電圧である。これらのうち、定格最大電圧は遮断し得る電圧の最大値である。

④ 電力機器の負荷は、一般に誘導性が多く、この場合遅れ力率による無効電力が発生する。このため、力率の改善を目的とした進相コンデンサが使用されている。

⑤ 受電用保護継電器は、過電流や過電圧による機器や電路の故障発生時に、故障区間を速やかに選択して遮断することにより、故障の波及防止と故障による損傷を最小限とすることを目的として使用されている。これらの主な方式には、誘導型継電器、電磁型継電器、静止型継電器などがある。

問３　次の問いに答えよ。　(小計２０点)

(１) 次の文章は、公衆電話網及びＩＳＤＮ網の加入者線区間における選択信号について述べたものである。［　　］内の(ア)～(エ)に最も適したものを、下記の解答群から選び、その番号を記せ。　(２点×４＝８点)

電話機と交換機間における選択信号の伝送方式には、ＤＰ信号方式とＰＢ信号方式がある。ＤＰ信号方式は、加入者線ループを選択数字に従った［（ア）］のパルスとなるよう断続させて数字情報を伝達する方式であり、ＰＢ信号方式と比較して、その伝達速度が遅い。

ＰＢ信号方式は、低群の［（イ）］周波数と高群の４周波数の中からそれぞれ１周波数ずつを組み合わせて、選択信号の数字やその他の符号を構成する方式である。ＰＢ信号は、［（ウ）］であるため、選択信号として使用する以外に、通話中のエンド・ツー・エンド信号としても使用可能である。

ＩＳＤＮ基本インタフェースでは、Ｄチャネルといわれる信号チャネルを通じて選択信号が伝送されており、選択数字は［（エ）］で表される。

<(ア)～(エ)の解答群>

① ２	② ３	③ ４	④ ８
⑤ 振　幅	⑥ 幅	⑦ 回　数	⑧ 可聴信号
⑨ ＢＣＨ符号		⑩ ＬＡＰＤ	
⑪ ４ビットのコード		⑫ ８ビットのコード	
⑬ 共通線信号方式		⑭ アウトチャネル信号	
⑮ ＭＦ信号方式と同一周波数			

(2) 次の文章は、ディジタル網における伝送品質の劣化要因と評価尺度について述べたものである。［　　］内の(オ)、(カ)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。
(3点×2＝6点)

(i) 伝送品質の劣化要因について述べた次のA～Cの文章は、［（オ）］。

A　伝送品質の劣化要因には、符号誤り、ジッタ、熱雑音、瞬断などがある。
B　符号誤りには、ランダム誤りと、バースト誤りがあり、ランダム誤りは、一般に、ランダム雑音、符号間干渉、雷などの外部からの誘導によるインパルス性雑音、無線伝送区間におけるフェージングなどによって発生する。
C　ジッタは、ディジタルパルス列の位相が短時間に揺らぐ現象のことであり、再生中継器のタイミング回路や多重化装置の同期回路等で発生する場合がある。

<(オ)の解答群>
① Aのみ正しい　② Bのみ正しい　③ Cのみ正しい
④ A、Bが正しい　⑤ A、Cが正しい　⑥ B、Cが正しい
⑦ A、B、Cいずれも正しい　⑧ A、B、Cいずれも正しくない

(ii) 伝送品質の評価尺度の一つである符号誤り時間率について述べた次のA～Cの文章は、［（カ）］。

A　符号誤り時間率は、一般に、稼働時間を除く時間に対して、単位時間T_0のなかの平均誤り率が、しきい値1×10^{-m}を超える各単位時間の数が、ある観測時間長T_Lに占める割合で表される。
B　稼働時間内における単位時間T_0を1秒、誤り率のしきい値1×10^{-m}を無限大、観測時間長T_Lを1か月とした場合の伝送品質測度は、一般に、%SESといわれる。
C　ITU－T勧告G.821において、国際ISDN接続(64kbit／s×N;N＝1～24)の%ESの品質目標許容値は、最長標準接続系に対して8〔%〕と規定されている。

<(カ)の解答群>
① Aのみ正しい　② Bのみ正しい　③ Cのみ正しい
④ A、Bが正しい　⑤ A、Cが正しい　⑥ B、Cが正しい
⑦ A、B、Cいずれも正しい　⑧ A、B、Cいずれも正しくない

(3) 次の文章は、生産性管理に関する用語について述べたものである。［　　］内の(キ)、(ク)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。なお、文章の内容は、ＪＩＳ　Ｚ８１４１を参考にしている。　　(3点×2＝6点)

(i) 設備効率及び設備更新に関する用語について述べた次の文章のうち、正しいものは、［(キ)］である。

<(キ)の解答群>

① 設備総合効率とは、設備の使用効率の度合を表す指標である。設備総合効率は、設備効率を阻害する停止ロスの大きさを表す時間稼働率と、不良ロスの大きさを表す良品率の積で表すことができる。

② 故障率とは、故障のために設備が停止した割合のことであり、故障強度率ともいう。

③ 保全費とは、設備保全に必要な費用であって、設備の新増設、更新、改造などの固定資産に繰り入れるべき費用、保全用予備品の在庫費用及び予備品を保有しておくためにかかる費用を除く費用のことである。

④ 劣化損失とは、設備劣化により設備が停止することによってもたらされる損失の総称である。

⑤ 資本回収期間法とは、設備投資の有効性又は安全性の判断に当たって、資本費用と操業費用の合計額が回収できる期間(年数)の長・短で設備投資案を評価・比較する方法のことをいう。

(ii) 設備管理について述べた次の文章のうち、誤っているものは、［(ク)］である。

<(ク)の解答群>

① 保全とは、故障の排除及び設備を正常・良好な状態に保つ活動の総称である。

② 劣化には、規定の運転条件又は使用条件の下で、運転又は使用によってストレスが加わり、設備の強度又は性能が劣っていく強制劣化がある。

③ 陳腐化とは、技術の進歩によって、所有している設備の技術レベル又は経済的価値が相対的に低下していく変化のことをいう。

④ 設備寿命とは、設備を導入し、使用を開始してから、廃棄又は更新するまでの期間のことをいう。

⑤ ライフサイクルとは、設備の計画、設計、製作、運用、保全を経て廃棄又は再利用までを含めたすべての段階及び期間のことをいう。

問４　次の問いに答えよ。　　(小計２０点)

(１)　次の文章は、費用による経済比較方法や設備の寿命について述べたものである。［　　］内の(ア)～(エ)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、［　　］内の同じ記号は、同じ解答を示す。　　(２点×４＝８点)

設備の新設などを行うに当たって、いくつかの案のうちから一つを選択する場合に、経済的な面から比較検討し、優劣を評価する方法がある。これらには、［(ア)］による比較方法、現価による比較方法などがある。

［(ア)］は、減価償却費と投下資金の使用料的な費用から成り立っている［(イ)］と、設備の維持・運用に必要な稼働費などの合計である。

設備などを取得してから、それが撤去又は廃棄されるなど、使われなくなるまでの期間を寿命という。寿命にはいくつかの種類がある。

設備の［(イ)］は使用期間が長くなるほど１年当たりの金額は少なくなる。一方、設備の維持・運用に必要な稼働費などは、一般に、使用期間が長くなるほど、１年当たりの費用は増加傾向を示す。

したがって、［(イ)］と稼働費などとの和は、ある適当な年数、ｎ年間使用したときに、［(ウ)］となる。この使用期間ｎ年を、［(エ)］寿命という。

<(ア)～(エ)の解答群>

①　運転資金	②　経　済	③　建設仮勘定費	④　最　小
⑤　最　大	⑥　残　価	⑦　資本回収費	⑧　実　用
⑨　設備投資	⑩　創設費	⑪　貯蔵品費	⑫　年経費
⑬　物理的	⑭　分　散	⑮　平　均	⑯　平均実用

(２)　次の文章は、ある装置Ａの信頼性について述べたものである。［　　］内の(オ)、(カ)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、装置Ａの故障の発生は指数分布に従うものとし、ＭＴＢＦは、５００〔時間〕とする。　　(３点×２＝６点)

装置Ａを修理しない条件で、ｎ〔台〕を１／ｎ冗長として並列に接続したシステムにおいて、このシステムのＭＴＴＦは、［(オ)］〔時間〕で求められる。

また、このシステムにおいて、ＭＴＴＦを１,０００〔時間〕以上にするためには、装置Ａを［(カ)］〔台〕以上並列に接続する必要がある。

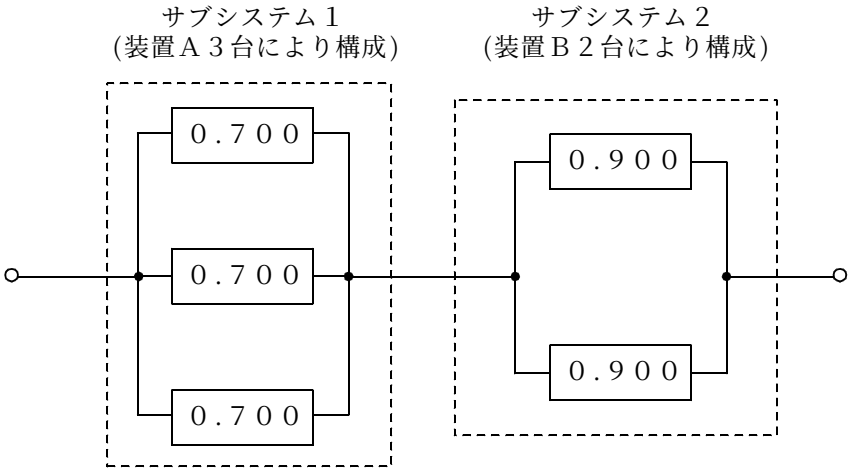
<(オ)、(カ)の解答群>

①　２　　②　３　　③　４　　④　５　　⑤　６　　⑥　７

⑦　$\left(1+\frac{1}{2}+\frac{1}{3}\cdot\cdot\cdot+\frac{1}{n}\right)\times 500$　　⑧　$\frac{500}{n}$

⑨　$n\times 500$

(３) 次の文章は、あるシステムの信頼度について述べたものである。 [　　] 内の(キ)、(ク)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、下図は信頼度に関する概念図であり、図中の [　　] 内の数字はそれぞれの構成装置の信頼度を示している。なお、答えは、四捨五入により小数第３位までとする。 (３点×２＝６点)



(ⅰ) 装置Ａ３台からなるサブシステム１が、多数決(２／３冗長構成)となっているときのサブシステム１の信頼度は、 [　(キ)　] である。

(ⅱ) 装置Ａ３台からなる多数決(２／３冗長構成)サブシステム１と装置Ｂ２台からなる二重化された(１／２冗長構成)サブシステム２とを接続した全体のシステムの信頼度は、 [　(ク)　] である。

<(キ)、(ク)の解答群>

① ０.７７６	② ０.７８４	③ ０.７８８	④ ０.８１０
⑤ ０.８８５	⑥ ０.９００	⑦ ０.９１０	⑧ ０.９６３
⑨ ０.９７０	⑩ ０.９７３	⑪ ０.９９０	⑫ ０.９９９

問５　情報セキュリティに関する次の問いに答えよ。　(小計２０点)

(１)　次の文章は、公開鍵基盤(ＰＫＩ)を用いた情報セキュリティについて述べたものである。［　　］内の(ア)～(エ)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、［　　］内の同じ記号は、同じ解答を示す。　(２点×４＝８点)

ＰＫＩは、公開鍵暗号方式を用いてディジタル署名、相手認証、メッセージ認証、安全な鍵配送などの機能を実現し、電子商取引や電子政府などのサービスを行うための基盤となるものである。

ＰＫＩは、［　(ア)　］をはじめとする幾つかの要素によって構成される。［　(ア)　］は、信頼できる第三者の認証機関ともいわれ、申請者に対して、鍵ペア(秘密鍵と公開鍵)の所持者であることの確認をした後、公開鍵証明書を発行する。公開鍵証明書には、一般に、ＩＴＵ－Ｔが規定した［　(イ)　］が標準として利用されており、［　(ア)　］の署名、証明書所有者、公開鍵情報などで構成されている。

［　(ウ)　］は、ＰＫＩを運用する範囲において、公開鍵証明書を発行する際の本人確認のための資格審査を行い、利用者登録などを行う。

ＶＡは、公開鍵証明書の有効性の検証やそれに付与された［　(ア)　］の署名が信頼できるものであるかどうかを判断する。公開鍵証明書には有効期限があり、期限切れや有効期限内での失効が生じた場合に、ＶＡは失効した公開鍵証明書を［　(エ)　］に登録する。

<(ア)～(エ)の解答群>

①　ＡＤ	②　ＳＡ	③　Ｘ.３２	④　ＣＲＬ
⑤　ＴＡ	⑥　ＣＰＳ	⑦　Ｘ.３２０	⑧　キャッシュ
⑨　ＣＡ	⑩　ＩＫＥ	⑪　Ｘ.５０１	⑫　Ｗｅｂサーバ
⑬　ＲＡ	⑭　ＴＳＡ	⑮　Ｘ.５０９	⑯　メールサーバ

(２)　ディジタル署名について述べた次の文章のうち、正しいものは、［　(オ)　］である。　(３点)

<(オ)の解答群>

①　ディジタル署名は、データの発信者特定による否認防止、改ざん検出や認証に広く利用されている。

②　Ｓ／ＭＩＭＥ等で用いられるＣＭＳは、共通鍵暗号を用いたＡＳＮ.１形式のディジタル署名フォーマットである。

③　ディジタル署名は、一般に、公開鍵暗号を用いる場合が多いが、不特定多数に対してディジタル署名を提供する場合には共通鍵暗号を用いることが多い。

④　ＤＳＡディジタル署名は、ＤＳＡ暗号の素因数分解問題の困難性を利用したもので、ハッシュアルゴリズムには、ＳＨＡ－１のみが用いられている。

⑤　ＲＳＡディジタル署名は、ＲＳＡ暗号の離散対数問題の困難性を利用したもので、ＲＳＡ暗号と同一の公開鍵を用いているため、公開鍵を公開すれば、暗号と署名の機能を同時に実現できる。

(３) 次の問いの [　　] 内の(カ)に適したものを、下記の解答群から選び、その番号を記せ。
(３点)

共通鍵暗号方式の特徴について述べた次のＡ～Ｃの文章は、 [(カ)] 。

Ａ　データを一定数のビットからなるブロックに区切り、ブロックごとに暗号化するブロック暗号は、一般には、ストリーム暗号と比較して高速処理が可能である。
Ｂ　共通鍵暗号方式は、公開鍵暗号方式と比較して、暗号化・復号化処理が速いことから、データ量の多い情報や映像情報の秘匿に向いている。
Ｃ　ストリーム暗号では、一般に、暗号強度は鍵の長さに大きく依存する。ブロック暗号の暗号強度は、擬似乱数発生器で完全乱数(乱数が予測不可能であること)に近い乱数を生成できるかに大きく依存している。

<(カ)の解答群>
① Ａのみ正しい　② Ｂのみ正しい　③ Ｃのみ正しい
④ Ａ、Ｂが正しい　⑤ Ａ、Ｃが正しい　⑥ Ｂ、Ｃが正しい
⑦ Ａ、Ｂ、Ｃいずれも正しい　⑧ Ａ、Ｂ、Ｃいずれも正しくない

(４) 次の問いの [　　] 内の(キ)に適したものを、下記の解答群から選び、その番号を記せ。
(３点)

ディジタルコンテンツの不正コピー対策技術について述べた次のＡ～Ｃの文章は、 [(キ)] 。

Ａ　なりすましによってコンテンツが不正な装置で受信できないように、装置の認証が行われることがある。装置認証は、専用端末の場合は出荷時に固有の秘密情報を組み込んでおく。パーソナルコンピュータの場合には、装置固有の情報としてＩＰアドレスを用いるか、何らかの事前手段によって秘密情報をパーソナルコンピュータに設定する。
Ｂ　受信したコンテンツを可搬媒体へ書き出す際には、コンテンツ受信者の指定に従って、コピーの可否、回数、範囲などを指定する情報がコンテンツに付加され、かつ、二次の不正コピー防止のためコンテンツを暗号化することが一般的である。
Ｃ　不正者によって著作権情報がコンテンツから除かれないように、データハイディング技術を用いて著作権情報をコンテンツに埋め込む方法がある。ただし、データハイディング技術では、一般に、コンテンツを劣化させないこと、画像処理や音響処理によって著作権情報が除去されないこと、という二つの要求を同時に満たす必要がある。

<(キ)の解答群>
① Ａのみ正しい　② Ｂのみ正しい　③ Ｃのみ正しい
④ Ａ、Ｂが正しい　⑤ Ａ、Ｃが正しい　⑥ Ｂ、Ｃが正しい
⑦ Ａ、Ｂ、Ｃいずれも正しい　⑧ Ａ、Ｂ、Ｃいずれも正しくない

(5) ファイル共有ソフトウェアＷｉｎｎｙ(ウィニー)について述べた次の文章のうち、正しいものは、 (ク) である。 (3点)

<(ク)の解答群>

① Ｗｉｎｎｙは、ピア・ツー・ピア(Ｐ２Ｐ)技術を用いており、中央サーバはファイル検索データベースの提供とユーザの接続管理などを行い、ファイルの情報は利用者間をバケツリレー式に転送される。

② Ｗｉｎｎｙの特徴としては、違法なデータがやり取りされていても監視や規制を行うことが事実上不可能で一元管理が困難であること、利用者が増加してもネットワークは混雑しないこと、などがある。

③ Ｗｉｎｎｙは、ユーザを指定したメッセージの送信、共有ファイルのリストの閲覧、共有ファイル中の特定ファイルを指定してのダウンロードはできない。

④ Ｗｉｎｎｙへのコンピュータウィルスの感染経路は、一般に、Ｐ２Ｐファイル共有ソフトウェアの共有フォルダ経由であり、メールの添付ファイル経由では感染しない。